

On the nuclei of a finite semifield

Giuseppe Marino and Olga Polverino

ABSTRACT. In this paper we collect and improve the techniques for calculating the nuclei of a semifield and we use these tools to determine the order of the nuclei and of the center of some commutative presemifields of odd characteristic recently constructed.

1. Introduction

Semifields are algebras satisfying all the axioms for a skewfield except (possibly) associativity of the multiplication. From a geometric point of view, semifields coordinatize certain translation planes (*semifield planes*) which are planes of Lenz–Barlotti class V (see, e.g., [16, Sec. 5.1]) and, by [1], the isomorphism relation between two semifield planes corresponds to the isotopism relation between the associated semifields. The first example of a finite semifield which is not a field was constructed by Dickson about a century ago in [19], using the term *nonassociative division ring*. These examples are commutative semifields of order q^{2k} and they exist for each q odd prime power and for each $k > 1$ odd. Since then and until 2008, the only other known families of commutative semifields of odd characteristic p , existing for each value of p , have been some Generalized twisted fields constructed by Albert in [2].

The relationship between commutative semifields of odd order and planar DO polynomials has given new impetus to construct new examples of such algebraic structures. Indeed in [33], [9], [6], [26], [7] and [34], several families of commutative semifields in odd characteristic have been constructed.

In this paper we collect and improve the results of the last years on techniques for calculating the nuclei of a semifield and we use these tools to determine the order of the nuclei and of the center of the semifields presented in [33], [9] and [6]. From these results we are able to prove that, when the order of the center is greater than 3, the Zha–Kyureghyan–Wang presemifields and the Budaghyan–Helleseth presemifields of [7] are new. Precisely, each Zha–Kyureghyan–Wang presemifield [33] is not isotopic to any Budaghyan–Helleseth presemifield [9] and both of them are not isotopic to any previously known presemifield. Also, using the same arguments we

1991 *Mathematics Subject Classification.* 12K10, 51A40.

Key words and phrases. Semifield, spread set, isotopy.

This work was supported by the Research Project of MIUR (Italian Office for University and Research) “Geometrie su Campi di Galois, piani di traslazione e geometrie di incidenza”.

show that the Bierbrauer presemifields [6] are isotopic to neither a Dickson semifield, nor to a Generalized twisted field and to any of the known presemifields in characteristic 3.

2. Isotopy relation and nuclei

A finite *semifield* $\mathbb{S} = (S, +, \star)$ is a finite binary algebraic structure satisfying all the axioms for a skewfield except (possibly) associativity of multiplication. The subsets of S

$$\mathbb{N}_l = \{a \in S \mid (a \star b) \star c = a \star (b \star c), \forall b, c \in S\},$$

$$\mathbb{N}_m = \{b \in S \mid (a \star b) \star c = a \star (b \star c), \forall a, c \in S\},$$

$$\mathbb{N}_r = \{c \in S \mid (a \star b) \star c = a \star (b \star c), \forall a, b \in S\}$$

and

$$\mathbb{K} = \{a \in \mathbb{N}_l \cap \mathbb{N}_m \cap \mathbb{N}_r \mid a \star b = b \star a, \forall b \in S\}$$

are fields and are known, respectively, as the *left nucleus*, *middle nucleus*, *right nucleus* and *center* of the semifield. A finite semifield is a vector space over its nuclei and its center.

If \mathbb{S} satisfies all axioms for a semifield except, possibly, the existence of an identity element for the multiplication then we call it a *presemifield*. The additive group of a presemifield is an elementary abelian p -group, for some prime p called the *characteristic* of \mathbb{S} .

Two presemifields, say $\mathbb{S} = (S, +, \star)$ and $\mathbb{S}' = (S', +, \star')$, with characteristic p , are said to be *isotopic* if there exist three invertible \mathbb{F}_p -linear maps g_1, g_2, g_3 from S to S' such that

$$g_1(x) \star' g_2(y) = g_3(x \star y)$$

for all $x, y \in S$; the triple (g_1, g_2, g_3) is an *isotopism* between \mathbb{S} and \mathbb{S}' . In each isotopy class of a presemifield we can find semifields (see [23, p. 204]). The sizes of the nuclei as well as the size of the center of a semifield are invariant under isotopy; for this reason we refer to them as the *parameters* of \mathbb{S} . Whereas, if \mathbb{S} is a presemifield, then the *parameters* of \mathbb{S} will be the parameters of any semifield isotopic to it. If $\mathbb{S} = (S, +, \star)$ is a presemifield, then $\mathbb{S}^d = (S, +, \star^d)$, where $x \star^d y = y \star x$ is a presemifield as well, and it is called the *dual* of \mathbb{S} . For a recent overview on the theory of finite semifields see Chapter 6 [24] in the collected work [15].

Let $\mathbb{S} = (S, +, \star)$ be a presemifield having characteristic p and order p^t . The set

$$\mathcal{C} = \{\varphi_y : x \in S \rightarrow x \star y \in S \mid y \in S\} \subset \mathbb{V} = \text{End}_{\mathbb{F}_p}(S)$$

is the *semifield spread set* associated with \mathbb{S} (*spread set* for short): \mathcal{C} is an \mathbb{F}_p -subspace of \mathbb{V} of rank t and each non-zero element of \mathcal{C} is invertible. Also, if \mathbb{S} is a semifield and e is the identity element of \mathbb{S} , then $id = \varphi_e \in \mathcal{C}$. It can be seen that, by translating the isotopy relation between presemifields in terms of the associated spread sets, just two maps of the triple (g_1, g_2, g_3) are involved. Indeed

Proposition 2.1. [28, Prop.2.1] *Let $\mathbb{S}_1 = (S_1, +, \bullet)$ and $\mathbb{S}_2 = (S_2, +, \star)$ be two presemifields and let \mathcal{C}_1 and \mathcal{C}_2 be the corresponding spread sets. Then \mathbb{S}_1 and \mathbb{S}_2 are isotopic under the isotopism (g_1, g_2, g_3) if and only if $\mathcal{C}_2 = g_3 \mathcal{C}_1 g_1^{-1} = \{g_3 \circ \varphi_y \circ g_1^{-1} \mid y \in S_1\}^1$.*

PROOF. Let $\mathcal{C}_1 = \{\varphi_y \mid y \in S_1\}$ and $\mathcal{C}_2 = \{\varphi'_y \mid y \in S_2\}$. The necessary condition can be easily proven. Indeed, if (g_1, g_2, g_3) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 , then $g_3(\varphi_y(x)) = \varphi'_{g_2(y)}(g_1(x))$ for each $x, y \in S_1$. Hence, $\varphi'_{g_2(y)} = g_3 \circ \varphi_y \circ g_1^{-1}$ for each $y \in S_1$ and the statement follows taking into account that $\mathcal{C}_2 = \{\varphi'_y \mid y \in S_2\} = \{\varphi'_{g_2(y)} \mid y \in S_1\}$.

Conversely, suppose that $\mathcal{C}_2 = \{g_3 \circ \varphi_y \circ g_1^{-1} \mid y \in S_1\}$, where g_1 and g_3 are invertible \mathbb{F}_p -linear maps from S_1 to S_2 . Then the map g_2 , sending each element $y \in S_1$ to the unique element $z \in S_2$ such that $\varphi'_z = g_3 \circ \varphi_y \circ g_1^{-1}$ (where $\varphi'_z \in \mathcal{C}_2$), is an invertible \mathbb{F}_p -linear map from S_1 to S_2 . Hence, for each $x, y \in S_1$ we get $\varphi'_{g_2(y)}(x) = g_3(\varphi_y(g_1^{-1}(x)))$, i.e. $x \star g_2(y) = g_3(g_1^{-1}(x) \bullet y)$ and putting $x' = g_1^{-1}(x)$ we have the assertion. \square

Move the study from the presemifield to the associated spread set, allows to determine its parameters without passing through an isotopic semifield.

The following result generalizes [29, Thm. 2.1].

Theorem 2.2. *Let $\mathbb{S} = (S, +, \star)$ be a presemifield of characteristic p and let \mathcal{C} be the associated spread set of \mathbb{F}_p -linear maps. Then*

- (1) *the right nucleus of each semifield isotopic to \mathbb{S} is isomorphic to the largest field $\mathcal{N}_r(\mathbb{S})$ contained in $\mathbb{V} = \text{End}_{\mathbb{F}_p}(S)$ such that $\mathcal{N}_r(\mathbb{S})\mathcal{C} \subseteq \mathcal{C}$;*
- (2) *the middle nucleus of each semifield isotopic to \mathbb{S} is isomorphic to the largest field $\mathcal{N}_m(\mathbb{S})$ contained in \mathbb{V} such that $\mathcal{C}\mathcal{N}_m(\mathbb{S}) \subseteq \mathcal{C}$;*
- (3) *the left nucleus of each semifield isotopic to \mathbb{S} is isomorphic to the largest field $\mathcal{N}_l(\mathbb{S})$ contained in \mathbb{V} such that $\mathcal{N}_l(\mathbb{S})\mathcal{C}^* \subseteq \mathcal{C}^*$, where \mathcal{C}^* is the spread set associated with the dual presemifield \mathbb{S}^* of \mathbb{S} ;*
- (4) *the center of each semifield isotopic to \mathbb{S} is isomorphic to the largest field $\mathcal{K}_{r,\omega}(\mathbb{S})$ contained in $\mathcal{N}_r(\mathbb{S})$ such that*

$$(2.1) \quad \rho \circ \varphi = \varphi \circ (\omega^{-1} \circ \rho \circ \omega)$$

for all $\rho \in \mathcal{K}_{r,\omega}(\mathbb{S})$ and $\varphi \in \mathcal{C}$, where ω is a fixed invertible element of \mathcal{C} . Equivalently, the center of each semifield isotopic to \mathbb{S} is isomorphic to the largest field $\mathcal{K}_{m,\sigma}(\mathbb{S})$ contained in $\mathcal{N}_m(\mathbb{S})$ such that

$$(2.2) \quad \varphi \circ \rho = (\sigma^{-1} \circ \rho \circ \sigma) \circ \varphi$$

for all $\rho \in \mathcal{K}_{m,\sigma}(\mathbb{S})$ and $\varphi \in \mathcal{C}$, where σ is a fixed invertible element of \mathcal{C} . Also, $\mathcal{K}_{m,\sigma}(\mathbb{S})$ and $\mathcal{K}_{r,\omega}(\mathbb{S})$ are conjugated fields.

PROOF. Let $\mathbb{S}' = (S', +, \bullet)$ be a semifield isotopic to \mathbb{S} and let \mathcal{C} and \mathcal{C}' be the associated spread sets. Then by the previous proposition, $\mathcal{C} = g_3 \mathcal{C}' g_1^{-1}$ for some invertible \mathbb{F}_p -linear maps from S' to S . If $\mathcal{N}_r(\mathbb{S}')$ is the right nucleus of \mathbb{S}' , then it is easy to see that $\mathcal{N}_r(\mathbb{S}') = \{\varphi_y : y \in \mathcal{N}_r(\mathbb{S}')\}$ is the maximum field contained in \mathbb{V} such that $\mathcal{N}_r(\mathbb{S}')\mathcal{C}' \subseteq \mathcal{C}'$, i.e. for each $\mu \in \mathcal{N}(\mathbb{S}')$ we have $\mu \circ \varphi'_y \in \mathcal{C}'$ for every $\varphi'_y \in \mathcal{C}'$, and, obviously, $\mathcal{N}_r(\mathbb{S}')$ is isomorphic to $\mathcal{N}_r(\mathbb{S}')$. Then, we have that

¹Here "o" stands for composition of maps.

$\mathcal{N}_r(\mathbb{S}')^{g_3^{-1}} := g_3 \mathcal{N}_r(\mathbb{S}') g_3^{-1}$ is the maximum field contained in \mathbb{V} with respect to which $\mathcal{N}_r(\mathbb{S}')^{g_3^{-1}} \mathcal{C} \subseteq \mathcal{C}$, i.e. $\mathcal{N}_r(\mathbb{S}) = \mathcal{N}_r(\mathbb{S}')^{g_3^{-1}}$, and, clearly, $\mathcal{N}_r(\mathbb{S})$ is isomorphic to $\mathbb{N}_r(\mathbb{S}')$. This shows our claim in Case (a). The same arguments can be used to prove point (b); in such a case we get that $\mathcal{N}_m(\mathbb{S}) = \mathcal{N}_m(\mathbb{S}')^{g_1^{-1}}$.

Now, noting that $\mathbb{N}_l(\mathbb{S}') = \mathbb{N}_r(\mathbb{S}'^d)$, applying point (a) to \mathbb{S}'^d , we get point (c).

Finally, let $\mathbb{K}(\mathbb{S}')$ be the center of \mathbb{S}' and note that $\mathcal{K}(\mathbb{S}') = \{\varphi'_y : y \in \mathbb{K}(\mathbb{S}')\}$ can be seen as the maximum subfield contained in $\mathcal{N}_r(\mathbb{S}')$ (or contained in $\mathcal{N}_m(\mathbb{S}')$) such that $\mu \circ \varphi' = \varphi' \circ \mu$ for each $\varphi' \in \mathcal{C}'$ and, obviously, $\mathcal{K}(\mathbb{S}')$ is isomorphic to $\mathbb{K}(\mathbb{S}')$.

Now, since $\mathcal{C} = g_3 \mathcal{C}' g_1^{-1}$, $\mathcal{N}_r(\mathbb{S}) = \mathcal{N}_r(\mathbb{S}')^{g_3^{-1}}$ and $\mathcal{N}_m(\mathbb{S}) = \mathcal{N}_m(\mathbb{S}')^{g_1^{-1}}$, we have that for each element $\rho \in \mathcal{K}(\mathbb{S}')^{g_3^{-1}}$ and for each $\varphi \in \mathcal{C}$

$$\rho \circ \varphi = \varphi \circ \rho^\omega$$

where $\omega = g_3 \circ g_1^{-1}$. Note that, since \mathbb{S}' is a semifield, ω is an element of \mathcal{C} . Now, it is easy to see that $\mathcal{K}(\mathbb{S}')^{g_3^{-1}}$ is the maximum subfield $\mathcal{K}_{r,\omega}(\mathbb{S})$ contained in $\mathcal{N}_r(\mathbb{S})$ satisfying (2.1). In the same way, we have that $\mathcal{K}(\mathbb{S}')^{g_1^{-1}}$ is the maximum subfield $\mathcal{K}_{m,\sigma}(\mathbb{S})$ contained in $\mathcal{N}_m(\mathbb{S})$ satisfying (2.2). \square

By the previous result it follows that we can define the middle nucleus (resp. right nucleus) of a presemifield $\mathbb{S} = (S, +, \star)$, with associated spread set \mathcal{C} , as the largest field contained in $\mathbb{V} = \text{End}_{\mathbb{F}_p}(S)$ with respect to which \mathcal{C} is a right vector space (resp. left vector space); similarly, the left nucleus of \mathbb{S} can be defined as the largest field contained in \mathbb{V} with respect to which \mathcal{C}^d (the spread set associated with the dual of \mathbb{S}) is a left vector space. Also, regarding the center, note that if \mathbb{S} is a semifield, then $id \in \mathcal{C}$ and hence

$$\mathcal{K}_{r,id}(\mathbb{S}) = \mathcal{K}_{m,id}(\mathbb{S}) = \mathcal{K}(\mathbb{S}) = \{\mu \in \mathcal{N}_r(\mathbb{S}) \cap \mathcal{N}_m(\mathbb{S}) : \mu \circ \varphi = \varphi \circ \mu \ \forall \varphi \in \mathcal{C}\}.$$

By the proof of the previous theorem we also have the following result.

Corollary 2.3. *If the presemifields \mathbb{S}_1 and \mathbb{S}_2 are isotopic via the isotopy (g_1, g_2, g_3) then*

- 1 $\mathcal{N}_r(\mathbb{S}_2) = g_3 \mathcal{N}_r(\mathbb{S}_1) g_3^{-1}$;
- 2 $\mathcal{N}_m(\mathbb{S}_2) = g_1 \mathcal{N}_m(\mathbb{S}_1) g_1^{-1}$;
- 3 $\mathcal{N}_l(\mathbb{S}_2) = g_3 \mathcal{N}_l(\mathbb{S}_1) g_3^{-1}$;
- 4 $\mathcal{K}_{r,\sigma}(\mathbb{S}_2) = g_3 \mathcal{K}_{r,\omega}(\mathbb{S}_1) g_3^{-1}$ and $\mathcal{K}_{m,\sigma}(\mathbb{S}_2) = g_1 \mathcal{K}_{m,\omega}(\mathbb{S}_1) g_1^{-1}$, where $\omega \in \mathcal{C}_1 \setminus \{0\}$ and $\sigma = g_3 \circ \omega \circ g_1^{-1} \in \mathcal{C}_2$.

2.1. The Knuth Chain. If $\mathbb{S} = (S, +, \star)$ is a presemifield n -dimensional over \mathbb{F}_p , and $\{e_1, \dots, e_n\}$ is an \mathbb{F}_p -basis for \mathbb{S} , then the multiplication can be written via the multiplication of the vectors e_i 's. Indeed, if $x = x_1 e_1 + \dots + x_n e_n$ and $y = y_1 e_1 + \dots + y_n e_n$, with $x_i, y_i \in \mathbb{F}_p$, then

$$(2.3) \quad x \star y = \sum_{i,j=1}^n x_i y_j (e_i \star e_j) = \sum_{i,j=1}^n x_i y_j \left(\sum_{k=1}^n a_{ijk} e_k \right)$$

for certain $a_{ijk} \in \mathbb{F}_p$, called the *structure constants* of \mathbb{S} with respect to the basis $\{e_1, \dots, e_n\}$. Knuth noted, in [23], that the action of the symmetric group \mathcal{S}_3 on the indices of the structure constants gives rise to another five presemifields starting from one presemifield \mathbb{S} . The set $[\mathbb{S}]$ of these (at most six) presemifields is called the *Knuth Chain* of \mathbb{S} , and consists of the presemifields $\{\mathbb{S}, \mathbb{S}^{(12)}, \mathbb{S}^{(13)}, \mathbb{S}^{(23)}, \mathbb{S}^{(123)}, \mathbb{S}^{(132)}\}$,

called the *derivatives* of \mathbb{S} (\mathbb{S} included).

In the same paper, the author proved that the action of \mathcal{S}_3 on the indices of the structure constants of a presemifield \mathbb{S} is well-defined with respect to the isotopism classes of \mathbb{S} , and by the *Knuth orbit* of \mathbb{S} we mean the set of isotopism classes corresponding to the Knuth chain \mathbb{S} .

The presemifield $\mathbb{S}^{(12)}$ is the *opposite algebra* of \mathbb{S} obtained by reversing the multiplication, or in other words, $\mathbb{S}^{(12)} = \mathbb{S}^d$, the dual of \mathbb{S} . Similarly, it is easy to see that the semifield $\mathbb{S}^{(23)}$ can be obtained by transposing the matrices corresponding to the transformations φ_y , $y \in \mathbb{S}$, with respect to some \mathbb{F}_p -basis of \mathbb{S} , and for this reason $\mathbb{S}^{(23)}$ is also denoted by \mathbb{S}^t , called the *transpose* of \mathbb{S} . With this notation, the Knuth orbit becomes $\{\mathbb{S}, [\mathbb{S}^d], [\mathbb{S}^t], [\mathbb{S}^{dt}], [\mathbb{S}^{td}], [\mathbb{S}^{dtd}]\}$. Note that t and d are operations of order two, i.e. $(\mathbb{S}^t)^t = \mathbb{S}$ and $(\mathbb{S}^d)^d = \mathbb{S}$.

It is possible to describe the transpose of a presemifield without fixing a basis of \mathbb{S} .

Let $\mathbb{S} = (S, +, \star)$ be a presemifield of characteristic p and order p^n , let $\mathbb{V} = \text{End}_{\mathbb{F}_p}(S)$ and let \mathcal{C} be the associated spread set. Denote by $\langle \cdot, \cdot \rangle$ a non-degenerate symmetric bilinear form of S as \mathbb{F}_p -vector space and denote by $\overline{\varphi}$ the adjoint of $\varphi \in \mathbb{V}$ with respect to $\langle \cdot, \cdot \rangle$, i.e. $\langle x, \varphi(y) \rangle = \langle \overline{\varphi}(x), y \rangle$ for each $x, y \in S$. Since the map $T : \varphi \in \mathbb{V} \mapsto \overline{\varphi} \in \mathbb{V}$ is an involutive antiautomorphism of the endomorphisms ring \mathbb{V} and $\dim \text{Ker} \varphi = \dim \text{Ker} \overline{\varphi}$, we get that $\overline{\mathcal{C}} = \{\overline{\varphi}_y : \varphi_y \in \mathcal{C}\}$ is an additive spread set as well, defining the presemifield $\overline{\mathbb{S}} = (S, +, \overline{\star})$ where $x \overline{\star} y = \overline{\varphi}_y(x)$ for each $x, y \in S$. It is possible to prove that $\overline{\mathbb{S}}$, up to isotopy, does not depend on the choice of the bilinear form $\langle \cdot, \cdot \rangle$ and that $\overline{\mathbb{S}}$ is isotopic to the presemifield \mathbb{S}^t . For this reason, in what follows, fixed a non-degenerate symmetric bilinear form $\langle \cdot, \cdot \rangle$ of S , the presemifield $\overline{\mathbb{S}}$, constructed by using the adjoints with respect to $\langle \cdot, \cdot \rangle$, will be denoted as \mathbb{S}^t and the associated spread set $\overline{\mathcal{C}}$ will be denoted as \mathcal{C}^t . Moreover, if X is a subset of \mathbb{V} , we will denote by \overline{X} the set of the adjoint maps, with respect to $\langle \cdot, \cdot \rangle$, of the elements of X .

Now, we are able to describe how the nuclei move in the Knuth chain (see also [27] and [25]).

Proposition 2.4. *If \mathbb{S} is a presemifield, then*

1. $\mathcal{N}_r(\mathbb{S}) = \mathcal{N}_l(\mathbb{S}^d) = \overline{\mathcal{N}_m(\mathbb{S}^t)}$;
2. $\mathcal{N}_m(\mathbb{S}) = \overline{\mathcal{N}_r(\mathbb{S}^t)} \cong \mathcal{N}_m(\mathbb{S}^d)$;
3. $\mathcal{N}_l(\mathbb{S}) = \mathcal{N}_r(\mathbb{S}^d) \cong \mathcal{N}_l(\mathbb{S}^t)$.

PROOF. Point 1. follows from Theorem 2.2 and from properties of the adjoint maps. Indeed, since T is an antiautomorphism, we get $T(\varphi \circ \mu) = T(\mu) \circ T(\varphi) = \overline{\mu} \circ \overline{\varphi}$ for each $\mu, \varphi \in \mathbb{V}$. The first part of 2. and 3. follows from 1.. Now, note that if μ is an element of $\mathcal{N}_m(\mathbb{S})$, then for each $y \in S$ there exists a unique element $z \in S$ such that $\varphi_y \circ \mu = \varphi_z$ and the map $\sigma_\mu : y \in S \mapsto z \in S$ is an invertible \mathbb{F}_p -linear map of S ; so, $F = \{\sigma_\mu : \mu \in \mathcal{N}_m(\mathbb{S})\}$ is a field of maps isomorphic to $\mathcal{N}_m(\mathbb{S})$ satisfying (b) of Theorem 2.2 relatively to \mathcal{C}^d , i.e. $\mathcal{N}_m(\mathbb{S}) \cong F = \mathcal{N}_m(\mathbb{S}^d)$. Finally, by using the previous relations and taking into account that $\mathbb{S}^{dtd} = \mathbb{S}^{tdt}$ we get

$$\mathcal{N}_\ell(\mathbb{S}^t) = \mathcal{N}_\ell(\mathbb{S}^{tdt}) = \overline{\mathcal{N}_m(\mathbb{S}^{tdt})} = \overline{\mathcal{N}_m(\mathbb{S}^{dtd})} \cong \mathcal{N}_r(\mathbb{S}^{dtt}) = \mathcal{N}_r(\mathbb{S}^d) = \mathcal{N}_\ell(\mathbb{S}).$$

□

2.2. Semifields and q -polynomials. If \mathbb{S} is a presemifield of characteristic p and order p^n , then we may assume, up to isomorphisms, that $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$, where $x \star y = F(x, y)$. Since $F(x, y)$ is additive with respect to both the variables x and y , it can be seen as the polynomial map associated with a p -polynomial of $\mathbb{F}_{p^n}[x, y]$, i.e.

$$F(x, y) = \sum_{i,j=0}^{n-1} a_{i,j} x^{p^i} y^{p^j}$$

where $a_{ij} \in \mathbb{F}_{p^n}$. Also, each element φ of $\mathbb{V} = \text{End}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ can be written in a unique way as $\varphi(x) = \sum_{i=0}^{n-1} \beta_i x^{p^i}$.

Now, let \langle, \rangle be the symmetric bilinear form of \mathbb{F}_{p^n} over \mathbb{F}_p defined by the following rule $\langle x, y \rangle = \text{tr}_{p^n/p}(xy)$. Then \langle, \rangle is a non-degenerate symmetric bilinear form and the adjoint $\bar{\varphi}$ of the element $\varphi(x) = \sum_{i=0}^{n-1} \beta_i x^{p^i}$ of \mathbb{V} with respect to \langle, \rangle , is $\bar{\varphi}(x) = \sum_{i=0}^{n-1} \beta_i^{p^{n-i}} x^{p^{n-i}}$. This implies that the dual and the transpose of \mathbb{S} are defined, respectively, by the following multiplications

$$x \star^d y = F(y, x)$$

and

$$x \star^t y = \sum_{i,j=0}^{n-1} a_{n-i,j}^{p^i} x^{p^i} y^{p^{i+j}},$$

where the indices i and j are considered modulo n .

The polynomial F defining the multiplication of \mathbb{S} can be useful to determine the order of the nuclei. In what follows, if \mathbb{F}_q is a subfield of \mathbb{F}_{p^n} , then we will denote by F_q the corresponding field of scalar maps $\{t_\lambda : x \in \mathbb{F}_{p^n} \mapsto \lambda x \in \mathbb{F}_{p^n} \mid \lambda \in \mathbb{F}_q\}$ contained in \mathbb{V} .

Theorem 2.5. *Let $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$ be a presemifield whose multiplication is given by $x \star y = F(x, y)$, with $F(x, y) = \sum_{i,j=0}^{n-1} a_{ij} x^{p^i} y^{p^j}$ and $a_{ij} \in \mathbb{F}_{p^n}$ and let \mathbb{F}_q be a subfield of \mathbb{F}_{p^n} .*

(A) *If there exists $\tau \in \text{Aut}(\mathbb{F}_q)$ such that*

$$F(\lambda x, y) = F(x, \lambda^\tau y) \quad \text{for each } x, y \in \mathbb{F}_{p^n} \text{ and for each } \lambda \in \mathbb{F}_q$$

then $\mathcal{N}_m(\mathbb{S})$ contains the field of maps F_q and $\mathcal{N}_m(\mathbb{S}) \subseteq \text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^n})$.

(B) *If the polynomial F is \mathbb{F}_q -semilinear with respect to y , then $\mathcal{N}_r(\mathbb{S})$ contains the field of maps F_q and $\mathcal{N}_r(\mathbb{S}) \subseteq \text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^n})$.*

(C) *If the polynomial F is \mathbb{F}_q -semilinear with respect to x , then $\mathcal{N}_l(\mathbb{S})$ contains the field of maps F_q and $\mathcal{N}_l(\mathbb{S}) \subseteq \text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^n})$.*

PROOF. Let us prove Statement (A). Recall that $\mathcal{N}_m(\mathbb{S})$ is the largest field contained in $\mathbb{V} = \text{End}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ such that $\mathcal{CN}_m(\mathbb{S}) \subseteq \mathcal{C}$. Let $\lambda \in \mathbb{F}_q$, then, for each $x, y \in \mathbb{F}_{p^n}$

$$\varphi_y \circ t_\lambda(x) = \varphi_y(\lambda x) = F(\lambda x, y) = F(x, \lambda^\tau y) = \varphi_{\lambda^\tau y}(x).$$

This means that for each $y \in \mathbb{F}_{p^n}$, $\varphi_y \circ t_\lambda = \varphi_{\lambda^\tau y} \in \mathcal{C}$, i.e. $\mathcal{C}F_q \subseteq \mathcal{C}$. Hence $F_q \subseteq \mathcal{N}_m(\mathbb{S})$ and since $(\mathcal{N}_m(\mathbb{S}), +, \circ)$ is a field, we get $\mu \circ t_\lambda = t_\lambda \circ \mu$ for each $\lambda \in \mathbb{F}_q$ and $\mu \in \mathcal{N}_m(\mathbb{S})$, i.e. $\mu \in \text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^n})$. Using similar arguments we can prove Statement (B).

Finally, let \mathcal{C}^d be the spread set associated with the dual presemifield \mathbb{S}^d of \mathbb{S} and let σ be the automorphism of \mathbb{F}_q associated with F with respect to the variable x , i.e. $F(\lambda x, y) = \lambda^\sigma F(x, y)$ for each $x, y \in \mathbb{F}_{p^n}$ and $\lambda \in \mathbb{F}_q$. Then, for each $\lambda \in \mathbb{F}_q$ and for each $x, y \in \mathbb{F}_{p^n}$ we have

$$t_\lambda \circ \varphi^x(y) = \lambda \varphi^x(y) = \lambda F(x, y) = F(\lambda^{\sigma^{-1}} x, y) = \varphi^{\lambda^{\sigma^{-1}} x}(y).$$

This means that for each $x \in \mathbb{F}_{p^n}$, $t_\lambda \circ \varphi^x = \varphi^{\lambda^{\sigma^{-1}} x} \in \mathcal{C}^d$, i.e. $F_q \mathcal{C}^d \subseteq \mathcal{C}^d$. It follows that $F_q \subseteq \mathcal{N}_\ell(\mathbb{S})$ and hence $\mathcal{N}_l(\mathbb{S}) \subseteq \text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^n})$. \square

Corollary 2.6. *Let $\mathbb{S} = (\mathbb{F}_{p^n}, +, \star)$ be a presemifield whose multiplication is given by $x \star y = F(x, y)$. If $F(x, y)$ is a q -polynomial (\mathbb{F}_q subfield of \mathbb{F}_{p^n}), i.e. $\mathcal{C}, \mathcal{C}^d \subseteq \text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^n})$, then*

$$F_q \subseteq \mathcal{N}_l(\mathbb{S}) \cap \mathcal{N}_m(\mathbb{S}) \cap \mathcal{N}_r(\mathbb{S}),$$

$$F_q \subseteq \mathcal{K}_{r,\omega}(\mathbb{S}) \cap \mathcal{K}_{m,\sigma}(\mathbb{S})$$

and

$$\mathcal{K}_{m,\sigma}, \mathcal{K}_{r,\omega}, \mathcal{N}_l(\mathbb{S}), \mathcal{N}_m(\mathbb{S}), \mathcal{N}_r(\mathbb{S}) \subseteq \text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^t})$$

for each $\omega, \sigma \in \mathcal{C} \setminus \{0\}$.

PROOF. It is sufficient to note that in this case we can write $F(x, y) = \sum_{i,j=0}^{h-1} a_{ij} x^{q^i} y^{q^j}$ with $a_{ij} \in \mathbb{F}_{p^n}$ and $q^h = p^n$. Then for each $\lambda \in \mathbb{F}_q$, we get $F(\lambda x, y) = \lambda F(x, y) = F(x, \lambda y)$ and hence by Theorem 2.5 and point (d) of Theorem 2.2, the assertion follows. \square

Recall that the dual and the transpose operations are invariant under isotopy. Hence it makes sense to ask which is the isotopism involving the duals and the transposes of two isotopic presemifields (see [28, Proposition 2.3]). Precisely, if \langle, \rangle is a given non-degenerate symmetric bilinear form of \mathbb{F}_{p^n} over \mathbb{F}_p and $\overline{\varphi}$ denotes the adjoint of $\varphi \in \mathbb{V}$ with respect to \langle, \rangle , then we can prove the following

Proposition 2.7. *Let $\mathbb{S}_1 = (\mathbb{F}_{p^n}, +, \bullet)$ and $\mathbb{S}_2 = (\mathbb{F}_{p^n}, +, \star)$ be two presemifields. Then*

- i) (g_1, g_2, g_3) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 if and only if (g_2, g_1, g_3) is an isotopism between the dual presemifields \mathbb{S}_1^d and \mathbb{S}_2^d ;
- ii) (g_1, g_2, g_3) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 if and only if $(\overline{g_3}^{-1}, g_2, \overline{g_1}^{-1})$ is an isotopism between the transpose presemifields \mathbb{S}_1^t and \mathbb{S}_2^t .

PROOF. Statement i) easily follows from the definition of dual operation.

Let us prove ii). Let $\mathcal{C}_1 = \{\varphi_y \mid y \in \mathbb{F}_{p^n}\}$ and $\mathcal{C}_2 = \{\varphi'_y \mid y \in \mathbb{F}_{p^n}\}$ be the corresponding spread sets. By the previous arguments the corresponding transpose presemifields are defined by the following multiplications $x \bullet^t y = \overline{\varphi_y}(x)$ and $x \star^t y = \overline{\varphi'_y}(x)$, respectively. The triple (g_1, g_2, g_3) is an isotopism between \mathbb{S}_1 and \mathbb{S}_2 if and only if $g_3 \circ \varphi_y = \varphi'_{g_2(y)} \circ g_1$ for each $y \in \mathbb{F}_{p^n}$. Since $\overline{\varphi_y} \circ \overline{g_3} = \overline{g_1} \circ \overline{\varphi'_{g_2(y)}}$ for each $y \in \mathbb{F}_{p^n}$, we have

$$\overline{g_3}(x) \bullet^t y = \overline{g_1}(x \star^t g_2(y))$$

for each $x, y \in \mathbb{F}_{p^n}$. This is equivalent to $\overline{g_1}^{-1}(z \bullet^t y) = \overline{g_3}^{-1}(z) \star^t g_2(y)$ for each $z, y \in \mathbb{F}_{p^n}$. So, the assertion follows. \square

Remark 2.8. If \mathbb{S}_1 and \mathbb{S}_2 are two isotopic presemifields, by using *i)* and *ii)* of the previous proposition, it is possible to determine the isotopisms between the other derivatives of \mathbb{S}_1 and \mathbb{S}_2 .

Finally, if two presemifields are both defined by \mathbb{F}_q -linear maps, then we have a restriction on the possible isotopisms between them (see [28, Thm. 2.2]).

Theorem 2.9. *If (g_1, g_2, g_3) is an isotopism between two presemifields \mathbb{S}_1 and \mathbb{S}_2 of order p^n , whose associated spread sets \mathcal{C}_1 and \mathcal{C}_2 are contained in $\text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^n})$ (\mathbb{F}_q a subfield of \mathbb{F}_{p^n}), then g_3 and g_1 are \mathbb{F}_q -semilinear maps of \mathbb{F}_{p^n} with the same companion automorphism.*

PROOF. Since $\mathcal{C}_1, \mathcal{C}_2 \subset \text{End}_{\mathbb{F}_q}(\mathbb{F}_{p^n})$, by Corollary 2.6, we have that

$$F_q \subset \mathcal{N}_l(\mathbb{S}_1) \cap \mathcal{N}_l(\mathbb{S}_2).$$

Also by Corollary 2.3, $\mathcal{N}_l(\mathbb{S}_2) = g_3 \mathcal{N}_l(\mathbb{S}_1) g_3^{-1}$. Then $g_3 F_q g_3^{-1} \subset \mathcal{N}_l(\mathbb{S}_2)$, and since a finite field contains a unique subfield of given order, it follows $g_3 F_q g_3^{-1} = F_q$. Hence the map $t_\lambda \mapsto g_3 t_\lambda g_3^{-1}$ is an automorphism of the field of maps F_q , and so there exists $i \in \{0, \dots, k-1\}$ such that $g_3 t_\lambda g_3^{-1} = t_{\lambda^{p^i}}$ (where $q = p^k$) for each $\lambda \in \mathbb{F}_q$, i.e. g_3 is an \mathbb{F}_q -semilinear map of \mathbb{F}_{p^n} with companion automorphism $\sigma(x) = x^{p^i}$. Finally, by Proposition 2.1, $g_3 \mathcal{C}_1 g_3^{-1} = \mathcal{C}_2$, and hence g_1 is an \mathbb{F}_q -semilinear map of \mathbb{F}_{p^n} as well, with the same companion automorphism σ . \square

3. The known families of commutative semifields

In 2003, Kantor in its article [22] pointed out as commutative semifields in odd characteristic, in particular when the characteristic is greater than 3, were very rare objects. Indeed until then the known examples of commutative proper² (pre)semifields of **odd order** were

D) Dickson semifields [18]: $(\mathbb{F}_{q^k} \times \mathbb{F}_{q^k}, +, \star)$, q odd and $k > 1$ odd, with

$$(a, b) \star (c, d) = (ac + j b^\sigma d^\sigma, ad + bc),$$

where j is a nonsquare in \mathbb{F}_{q^k} , σ is an \mathbb{F}_q -automorphism of \mathbb{F}_{q^k} , $\sigma \neq id$. These presemifields have middle nucleus of order q^k and center of order q (see [17], [18], [19]).

A) Generalized twisted fields [2]: $(\mathbb{F}_{q^t}, +, \star)$, q odd and $t > 1$ odd, with

$$x \star y = x^\alpha y + xy^\alpha,$$

where $\alpha : x \mapsto x^{q^n}$ is automorphism of \mathbb{F}_{q^t} , with $\text{Fix } \sigma = \mathbb{F}_q$ and $\frac{t}{\gcd(t, n)}$ is odd. These presemifields have middle nucleus and center both of order q (see [3]).

G) Ganley semifields [21]: $(\mathbb{F}_{3^r} \times \mathbb{F}_{3^r}, +, \star)$, $r \geq 3$ odd, with

$$(a, b) \star (c, d) = (ac - b^9 d - bd^9, ad + bc + b^3 d^3).$$

These semifields have middle nucleus and center both of order 3.

CG) Cohen–Ganley semifields [11]: $(\mathbb{F}_{3^s} \times \mathbb{F}_{3^s}, +, \star)$, $s \geq 3$, with

$$(a, b) \star (c, d) = (ac + jbd + j^3(bd)^9, ad + bc + j(bd)^3)$$

where j is a nonsquare in \mathbb{F}_{3^s} . These semifields have middle nucleus of order 3^s and center of order 3.

²Here a presemifield is called *proper* if it not isotopic to a field

$\mathcal{CM}/\mathcal{DY}$) *Coulter–Matthews/Ding–Yuan presemifields* [14], [20]: $(\mathbb{F}_{3^e}, +, \star)$, $e \geq 3$ odd, with

$$x \star y = x^9 y + xy^9 \pm 2x^3 y^3 - 2xy.$$

Arguing as in the proof of Theorem 4.5, straightforward computations show that the $\mathcal{CM}/\mathcal{DY}$ presemifields have nuclei and center all of order 3. In [12], the authors have showed that, for each $e \geq 5$ odd, these two presemifields are not isotopic and they are not isotopic to any previously known commutative semifield.

$\mathcal{PW}/\mathcal{BLP}$) *Penttila–Williams/Bader–Lunardon–Pinneri semifield* [31], [4]: $(\mathbb{F}_{3^5} \times \mathbb{F}_{3^5}, +, \star)$, with

$$(a, b) \star (c, d) = (ac + (bd)^9, ad + bc + (bd)^{27}).$$

This commutative semifield arises from the symplectic semifield associated with the Penttila–Williams translation ovoid of $Q(4, 3^5)$. The $\mathcal{PW}/\mathcal{BLP}$ semifield has middle nucleus of order 3^5 and center of order 3.

\mathcal{CHK}) *Coulter–Henderson–Kosick presemifield* [13]: $(\mathbb{F}_{3^8}, +, \star)$, with

$$x \star y = xy + L(xy^9 + x^9 y - xy - x^9 y^9) + x^{243} y^3 + x^{81} y - x^9 y + x^3 y^{243} + xy^{81} - xy^9,$$

where $L(x) = x^{3^5} + x^{3^2}$. This presemifield has middle nucleus of order 3^2 and center of order 3.

Note that two (pre)semifields belonging to different families of the previous list are not isotopic.

In the last years some other commutative semifields have been constructed, precisely:

\mathcal{ZKW}) *Zha–Kyureghyan–Wang presemifields* [33], [5, Thm. 4]: $(\mathbb{F}_{p^{3s}}, +, \star)$, with

$$x \star y = y^{p^t} x + yx^{p^t} - u^{p^s-1}(y^{p^{s+t}} x^{p^{2s}} + y^{p^{2s}} x^{p^{s+t}}),$$

where u is a primitive element of $\mathbb{F}_{p^{3s}}$ and $0 < t < 3s$ such that $\frac{s}{\gcd(s,t)}$ is odd and

$$(3.1) \quad \frac{s}{\gcd(s,t)} + \frac{t}{\gcd(s,t)} \equiv 0 \pmod{3}.$$

In [33, Cor. 1], it has been proven that, if $p \geq 5$, s is odd and $t \neq 2s$, these presemifields are not isotopic to any previously know presemifield listed above. In [26, Cor. 3] the same result has been obtained also when s is even.

In [6], the author has proven that the previous multiplication gives rise to a commutative presemifield if, instead of Condition (3.1), the following condition is fulfilled

$$(3.2) \quad p^s \equiv p^t \equiv 1 \pmod{3}.$$

Moreover, in [5, Thm. 7] it has shown that, when $p \equiv 1 \pmod{3}$ these presemifields are not isotopic to a Generalized twisted field.

\mathcal{B}) *Bierbrauer presemifields* [6]: $(\mathbb{F}_{p^{4s}}, +, \star)$, p odd prime, with

$$x \star y = y^{p^t} x + yx^{p^t} - u^{p^s-1}(y^{p^{s+t}} x^{p^{3s}} + y^{p^{3s}} x^{p^{s+t}}),$$

where u is a primitive element of $\mathbb{F}_{p^{4s}}$ and $0 < t < 4s$ such that $\frac{2s}{\gcd(2s,t)}$ is odd and $p^s \equiv p^t \equiv 1 \pmod{4}$. In [6, Thm. 7], it has been proven that, if

$t = 2$ and $s > 1$, these presemifields are not isotopic neither to a Dickson semifield nor to a Generalized twisted field.

In [9], two families of commutative presemifields of order p^{2m} , p odd prime, are constructed starting from certain Perfect Nonlinear DO-polynomials over $\mathbb{F}_{p^{2m}}$ labeled as (i^*) and (ii^*) . In [10, Thm. 3] it has been shown that the middle nucleus of the presemifields of type (i^*) has square order. In this way the authors have proven that for $p \neq 3$ and m odd the commutative presemifields of type (i^*) are new ([10, Cor. 8]). Later on, in [7], these presemifields are simplified. More precisely, the author proves that these two families of presemifields are contained, up to isotopy, into the following family

\mathcal{BH}) *Budaghyan–Helleseth presemifields* [9], [7]: $(\mathbb{F}_{p^{2m}}, +, \star)$, p odd prime and $m > 1$, with

$$(3.3) \quad x \star y = xy^{p^m} + x^{p^m}y + [\beta(xy^{p^s} + x^{p^s}y) + \beta^{p^m}(xy^{p^s} + x^{p^s}y)^{p^m}]\omega,$$

where $0 < s < 2m$, ω is an element of $\mathbb{F}_{q^{2m}} \setminus \mathbb{F}_{q^m}$ with $\omega^{q^m} = -\omega$ and the following conditions are satisfied:

(3.4)

$$\beta \in \mathbb{F}_{p^{2m}}^* : \beta^{\frac{p^{2m}-1}{(p^m+1, p^s+1)}} \neq 1 \quad \text{and} \quad \nexists a \in \mathbb{F}_{p^{2m}}^* : a + a^{p^m} = a + a^{p^s} = 0.$$

Also in [7], the author presents the family of commutative semifields

\mathcal{LMPTB}) *P*(q, ℓ) *semifields* [7]: $(\mathbb{F}_{q^{2\ell}}, +, \star)$, q odd prime power and $\ell = 2k + 1 > 1$ odd, with

$$x * y = \frac{1}{2}(xy + x^{q^\ell}y^{q^\ell}) + \frac{1}{4}G(xy^{q^2} + x^{q^2}y),$$

$$\text{where } G(x) = \sum_{i=1}^k (-1)^i (x - x^{q^\ell})^{q^{2i}} + \sum_{j=1}^{k-1} (-1)^{k+j} (x - x^{q^\ell})^{q^{2j+1}}.$$

These semifields generalize the semifields constructed in [26], which have order q^6 , middle nucleus of order q^2 and center of order q ([26, Thm. 8]). In [7] it has been proven that \mathcal{LMPTB} is not isotopic to any previously known semifield with the possible exception of \mathcal{BH} presemifields. Indeed, it has been recently proven, in [28], that each \mathcal{LMPTB} semifield is isotopic to a \mathcal{BH} presemifield.

The aim of this paper is to study the isotopy relation involving the commutative presemifields listed above. In order to do this, a very useful tool will be the computation of the order of their middle nucleus and their center. (Recall that, if a presemifield is isotopic to a commutative semifield \mathbb{S} , then $\mathbb{N}_\ell(\mathbb{S}) = \mathbb{N}_r(\mathbb{S}) = \mathcal{K}(\mathbb{S})$.)

4. The isotopy issue

In this section we want to face with the isotopy issue between the presemifields listed in the previous section. In order to do this we first compute the nuclei of the involved presemifields.

4.1. The nuclei of \mathcal{BH} presemifields. Let p be an odd prime, m and s two positive integers such that $0 < s < 2m$. Let ω be an element of $\mathbb{F}_{p^{2m}} \setminus \mathbb{F}_{p^m}$ with $\omega^{p^m} = -\omega$, the Budaghyan–Helleseth presemifields presented in [7] are defined by Multiplication (3.3) under Conditions (3.4).

Set $h := \gcd(m, s)$, then $m = h\ell$ and $s = hd$, where ℓ and d are two positive integers such that $0 < d < 2\ell$ and $\gcd(\ell, d) = 1$. Putting $q = p^h$, then $\omega \in \mathbb{F}_{q^{2\ell}} \setminus \mathbb{F}_{q^\ell}$ and $\omega^{q^\ell} = -\omega$ and the Budaghyan–Helleseth presemifields $BH(p, m, s, \beta)$

will be denoted by $\overline{BH}(q, \ell, d, \beta) = (\mathbb{F}_{q^{2\ell}}, +, \star)$. Moreover, Multiplication (3.3) and Conditions (3.4) can be rewritten as

$$(4.1) \quad x \star y = xy^{q^\ell} + x^{q^\ell}y + [\beta(xy^{q^d} + x^{q^d}y) + \beta^{q^\ell}(xy^{q^d} + x^{q^d}y)^{q^\ell}]\omega,$$

where

$$(4.2) \quad \beta \in \mathbb{F}_{q^{2\ell}}^* : \quad \beta^{\frac{q^{2\ell}-1}{(q^\ell+1, q^d+1)}} \neq 1,$$

and

$$(4.3) \quad \nexists a \in \mathbb{F}_{q^{2\ell}}^* : \quad a + a^{q^\ell} = a + a^{q^d} = 0.$$

Referring to Multiplication (4.1) for the two families of commutative presemifields of type (i^*) and (ii^*) presented in [9], it has been proven that in both cases their middle nucleus always contains a field of order q (see [10, Prop. 5 and Prop. 7]). Indeed we will prove that it has order q^2 .

In [28, Sec. 3] it has been proved that (4.2) and (4.3) are equivalent to

$$(4.4) \quad \ell + d \text{ odd}$$

and

$$(4.5) \quad \beta \text{ nonsquare in } \mathbb{F}_{q^{2\ell}}.$$

Now we can prove

Theorem 4.1. *A $\overline{BH}(q, \ell, d, \beta)$ presemifield of order $q^{2\ell}$, q an odd prime power and $\ell > 1$, has middle nucleus of order q^2 and right nucleus, left nucleus and center all of order q .*

PROOF. Recall that $0 < d < 2\ell$ with $\ell + d$ odd and $\gcd(\ell, d) = 1$. Set $x \circ_r y = xy^{q^r} + x^{q^r}y$ for any integer $0 < r < 2\ell$, then

$$(4.6) \quad \mathcal{C} = \{\varphi_y : x \mapsto x \circ_\ell y + [\beta(x \circ_d y) + \beta^{q^\ell}(x \circ_d y)^{q^\ell}]\omega \mid y \in \mathbb{F}_{q^{2\ell}}\}$$

is the spread set associated with the presemifield $\overline{BH}(q, \ell, d, \beta)$. In particular \mathcal{C} is contained in the vector space $\mathbb{V} = \text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^{2\ell}})$.

By (b) of Theorem 2.2 and by (A) of Theorem 2.5, the middle nucleus of $\overline{BH}(q, \ell, d, \beta)$ is isomorphic to the largest field, say $\mathcal{N}_m(\mathbb{S})$, contained in the space \mathbb{V} and satisfying the property $\varphi_y \circ \psi \in \mathcal{C}$, for each $\varphi_y \in \mathcal{C}$ and for each $\psi \in \mathcal{N}_m(\mathbb{S})$. This is equivalent to say that for each $x, y \in \mathbb{F}_{q^{2\ell}}$ there exists an element $z \in \mathbb{F}_{q^{2\ell}}$ such that $\varphi_y(\psi(x)) = \varphi_z(x)$, i.e. there exists $z \in \mathbb{F}_{q^{2\ell}}$ such that

$$\psi(x) \circ_\ell y + [\beta(\psi(x) \circ_d y) + \beta^{q^\ell}(\psi(x) \circ_d y)^{q^\ell}]\omega = x \circ_\ell z + [\beta(x \circ_d z) + \beta^{q^\ell}(x \circ_d z)^{q^\ell}]\omega$$

for each $x, y \in \mathbb{F}_{q^{2\ell}}$. Since $\{1, \omega\}$ is an \mathbb{F}_{q^ℓ} -basis of $\mathbb{F}_{q^{2\ell}}$, this is equivalent to show there exists $z \in \mathbb{F}_{q^{2\ell}}$ such that for each $x, y \in \mathbb{F}_{q^{2\ell}}$ the following system

$$(4.7) \quad \begin{cases} \psi(x) \circ_\ell y = x \circ_\ell z \\ \beta(\psi(x) \circ_d y) + \beta^{q^\ell}(\psi(x) \circ_d y)^{q^\ell} = \beta(x \circ_d z) + \beta^{q^\ell}(x \circ_d z)^{q^\ell} \end{cases}$$

admits solutions. Since $\psi \in \mathbb{V} = \text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^{2\ell}})$, we have $\psi(x) = \sum_{i=0}^{2\ell-1} a_i x^{q^i}$, with $a_i \in \mathbb{F}_{q^{2\ell}}$ and looking at the first equation of System (4.7) we get

$$\left(\sum_i a_i x^{q^i}\right)y^{q^\ell} + \left(\sum_i a_i^{q^\ell} x^{q^{i+\ell}}\right)y = xz^{q^\ell} + x^{q^\ell}z,$$

for each $x, y \in \mathbb{F}_{q^{2\ell}}$. Hence, reducing the above equation modulo $x^{q^{2\ell}} - x$, we have that for each $y \in \mathbb{F}_{q^{2\ell}}$ there exists $z \in \mathbb{F}_{q^{2\ell}}$ such that

$$a_i y^{q^\ell} + a_{i+\ell}^{q^\ell} y = \begin{cases} 0 & \text{if } i \neq 0, \ell \\ z^{q^\ell} & \text{if } i = 0 \\ z & \text{if } i = \ell \end{cases}$$

where $a_i = a_j$ if and only if $i \equiv j \pmod{2\ell}$. From the last equalities we get that $a_i = 0$ for each $i \neq 0, \ell$ and $z = a_0^{q^\ell} y + a_\ell y^{q^\ell}$. Hence, from the first equation of System (4.7), it follows that if $\psi \in \mathcal{N}_m(\mathbb{S})$, then $\psi(x) = \psi_{A,B}(x) = Ax + Bx^{q^\ell}$, with $A, B \in \mathbb{F}_{q^{2\ell}}$, and $z = A^{q^\ell} y + B y^{q^\ell}$ for each $y \in \mathbb{F}_{q^{2\ell}}$. Substituting these conditions in the second equation of (4.7), we get that for each $x, y \in \mathbb{F}_{q^{2\ell}}$ the following polynomial identity must be satisfied

$$\beta((Ax + Bx^{q^\ell}) \circ_d y) + \beta^{q^\ell}((Ax + Bx^{q^\ell}) \circ_d y)^{q^\ell} = \beta(x \circ_d (A^{q^\ell} y + B y^{q^\ell})) + \beta^{q^\ell}(x \circ_d (A^{q^\ell} y + B y^{q^\ell}))^{q^\ell}.$$

Reducing modulo $x^{q^{2\ell}} - x$ and equating the coefficients of the obtained reduced polynomials we have that A and B must verify the system

$$\begin{cases} \beta A = \beta A^{q^{\ell+d}} \\ \beta B = \beta^{q^\ell} B^{q^{\ell+d}}. \end{cases}$$

Note that, since $\gcd(2\ell, \ell + d) = \gcd(\ell, d) = 1$ the set of solutions in $\mathbb{F}_{q^{2\ell}}$ of the equations $x^{q^{\ell+d}-1} = 1$ is the set of nonzero elements of \mathbb{F}_q . Hence, taking into account that $\beta \neq 0$ and $(\beta^{q^\ell-1})^{\frac{q^{2\ell}-1}{q-1}} = 1$, we get

$$A \in \mathbb{F}_q \quad \text{and} \quad B = b\xi,$$

where $b \in \mathbb{F}_q$ and ξ is an element of $\mathbb{F}_{q^{2\ell}}$ such that $\xi^{q^{\ell+d}-1} = \beta^{1-q^\ell}$. It follows that

$$\mathcal{N}_m(\mathbb{S}) = \{\psi_{a,b\xi} : x \mapsto ax + b\xi x^{q^\ell} \mid a, b \in \mathbb{F}_q\},$$

and hence the middle nucleus of the presemifield $\overline{BH}(q, \ell, d, \beta)$ has order q^2 .

On the other hand, by (a) of Theorem 2.2 and by (B) of Theorem 2.2, the right nucleus of $\overline{BH}(q, \ell, d, \beta)$ is isomorphic to the largest field, say $\mathcal{N}_r(\mathbb{S})$, of the space $\mathbb{V} = \text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^{2\ell}})$, whose elements $\phi: x \mapsto \sum_{i=0}^{2\ell-1} a_i x^{q^i}$, with $a_i \in \mathbb{F}_{q^{2\ell}}$, satisfy the property $\phi \circ \varphi_y \in \mathcal{C}$, for each $\varphi_y \in \mathcal{C}$. Arguing as above we get that $\mathcal{N}_r(\mathbb{S}) = \{x \mapsto ax \mid a \in \mathbb{F}_q\}$. Since a presemifield $\overline{BH}(q, \ell, d, \beta)$ is commutative, then its left nucleus and its center have both order q .

Now the statement has been completely proven. \square

Corollary 4.2. *Each LMPTB semifield of order $q^{2\ell}$, q odd prime and $\ell > 1$ odd, has middle nucleus of order q^2 and right nucleus, left nucleus and center all of order q .*

PROOF. It follows from Theorem 4.1 and by [28, Thm. 4.5]. \square

Recall that in [10, Cor. 8] the authors have proven that some \mathcal{BH} presemifields of order p^{2m} , $p > 3$ odd prime and m odd are isotopic nor to a Dickson semifield nor to a Generalized twisted field and, obviously, nor to a presemifield of characteristic 3. By using the previous theorem we can now prove a stronger result.

Corollary 4.3. *A $\overline{BH}(q, 2, d, \beta)$ presemifield of order q^4 , q an odd prime power, with Multiplication (4.1), is isotopic to a Dickson semifield.*

A $\overline{BH}(q, \ell, d, \beta)$ presemifield of order $q^{2\ell}$, q an odd prime power and $\ell > 2$, with Multiplication (4.1), is isotopic nor to a Dickson semifield nor to a Generalized twisted field.

PROOF. If $\ell = 2$, from Theorem 4.1 each $\overline{BH}(q, \ell, d, \beta)$ presemifield is 2-dimensional over its middle nucleus and 4-dimensional over its center. Hence it is isotopic to a Dickson semifield (see [32], [8]). If $\ell > 2$, by Theorem 4.1, comparing the dimensions of the involved presemifields over their middle nucleus and over their center (see Table 1), we get the assertion. \square

4.2. The nuclei of Bierbrauer presemifields. Set $h = \gcd(s, t)$, then $s = hm$ and $t = hn$ with $\gcd(m, n) = 1$. Then the multiplication of a Bierbrauer presemifield $\mathbb{B} = (\mathbb{F}_{q^{4m}}, +, \star)$, $q = p^h$ odd prime power, can be rewritten as

$$(4.8) \quad x \star y = y^{q^n} x + y x^{q^n} - v(y^{q^{m+n}} x^{q^{3m}} + y^{q^{3m}} x^{q^{m+n}}),$$

where $v = u^{q^m - 1}$, u a primitive element of $\mathbb{F}_{q^{4m}}$, and $0 < n < 4m$ such that $\frac{2m}{\gcd(2m, n)}$ is odd and $q^m \equiv q^n \equiv 1 \pmod{4}$.

Remark 4.4. Since $\frac{2m}{\gcd(2m, n)}$ is odd and $\gcd(m, n) = 1$, n is even and m is odd. It follows that Condition $q^n \equiv 1 \pmod{4}$ is satisfied for each q odd, whereas Condition $q^m \equiv 1 \pmod{4}$ is equivalent to $q \equiv 1 \pmod{4}$.

In [6, Thm. 6] it has been proven that a \mathcal{B} presemifield of order q^{4m} , q odd prime power, has middle nucleus containing a field of order q^2 and center containing \mathbb{F}_q . Moreover, if q is prime, $n = 2$ and $m > 1$ odd, a \mathcal{B} presemifield is not quadratic over its middle nucleus ([6, Thm. 7]). Finally, if $q = p$ is an odd prime, $m = 3$ and $n = 2$, a \mathcal{B} presemifield has middle nucleus of order p^2 and center of order p ([5, Thm. 6]).

Here we determine the orders of the nuclei and the center of the involved presemifields, with no restriction on n , m or q .

Theorem 4.5. *A Bierbrauer presemifield $\mathbb{B} = (\mathbb{F}_{q^{4m}}, +, \star)$, q an odd prime power, with Multiplication (4.8), has middle nucleus of order q^2 and center of order q .*

PROOF. Let $\mathcal{C} = \{\varphi_y : x \mapsto x \star y \mid y \in \mathbb{F}_{q^{4m}}\} \subset \mathbb{V} = \text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^{4m}})$ be the spread set associated with the semifield \mathbb{B} . Note that if $x \star y = F(x, y)$, then $F(\lambda x, y) = F(x, \lambda y)$ for each $\lambda \in \mathbb{F}_{q^2}$. Hence, by (A) of Theorem 2.5, we get that the middle nucleus of \mathbb{B} is the largest field $\mathcal{N}_m(\mathbb{B})$ contained the field of maps F_{q^2} and contained in the space $\text{End}_{\mathbb{F}_{q^2}}(\mathbb{F}_{q^{4m}})$ satisfying the property $\varphi_y \circ \psi \in \mathcal{C}$, for each $\varphi_y \in \mathcal{C}$ and $\psi \in \mathcal{N}_m(\mathbb{B})$. This is equivalent to say that for each $x, y \in \mathbb{F}_{q^{4m}}$ there exists an element $z \in \mathbb{F}_{q^{4m}}$ such that $\varphi_y(\psi(x)) = \varphi_z(x)$, where $\psi(x) = \sum_{i=0}^{2m-1} a_i x^{q^{2i}}$, with $a_i \in \mathbb{F}_{q^{4m}}$, i.e.

$$(4.9) \quad y \sum_i a_i^{q^n} x^{q^{n+2i}} + y^{q^n} \sum_i a_i x^{q^{2i}} - v \left(y^{q^{m+n}} \sum_i a_i^{q^{3m}} x^{q^{3m+2i}} + y^{q^{3m}} \sum_i a_i^{q^{m+n}} x^{q^{2i+m+n}} \right) = z^{q^n} x + z x^{q^n} - v(z^{q^{m+n}} x^{q^{3m}} + z^{q^{3m}} x^{q^{m+n}}),$$

for each $x, y \in \mathbb{F}_{q^{4m}}$.

Now, reduce the above polynomials modulo $x^{q^{4m}} - x$ and equate the coefficients. Since the monomials $x, x^{q^n}, x^{q^{3m}}, x^{q^{m+n}}$ are pairwise distinct modulo $x^{q^{4m}} - x$, $n+m$ is odd and $\gcd(n, m) = 1$, we get

$$a_{i-\frac{n}{2}}^{q^n} y + a_i y^{q^n} = \begin{cases} z^{q^n} & \text{if } i = 0 \\ z & \text{if } 2i = n \\ 0 & \text{otherwise} \end{cases} \quad \begin{matrix} (a) \\ (b) \end{matrix}$$

for all $y \in \mathbb{F}_{q^{4m}}$, where $a_j = a_{j'}$ if and only if $j \equiv j' \pmod{4m}$. From the previous equalities we get

$$(4.10) \quad a_i = a_{i-\frac{n}{2}} = 0 \quad \forall i \notin \left\{0, \frac{n}{2}\right\} \pmod{4m}.$$

Combining (a) and (b) we get

$$(4.11) \quad a_{4m-\frac{n}{2}}^{q^n} y + a_0 y^{q^n} = a_0^{q^{2n}} y^{q^n} + a_{\frac{n}{2}}^{q^n} y^{q^{2n}}.$$

Hence

$$(4.12) \quad a_{\frac{n}{2}} = a_{4m-\frac{n}{2}} = 0$$

and

$$(4.13) \quad a_0 = a_0^{q^{2n}} \quad \text{and} \quad z = a_0^{q^n} y.$$

By using (4.10), (4.12) and (4.13) in Equation (4.9), we get that for each $x, y \in \mathbb{F}_{q^{4m}}$ there exists $z \in \mathbb{F}_{q^{4m}}$ such that

$$\begin{aligned} & a_0 y^{q^n} x + a_0^{q^n} y x^{q^n} - v(a_0^{q^{3m}} y^{q^{m+n}} x^{q^{3m}} + a^{q^{m+n}} y^{q^{3m}} x^{q^{m+n}}) = \\ & = a_0^{q^{2n}} y^{q^n} x + a_0^{q^n} y x^{q^n} - v(a_0^{q^{m+2n}} y^{q^{m+n}} x^{q^{3m}} + a_0^{q^{3m+n}} y^{q^{3m}} x^{q^{m+n}}), \end{aligned}$$

which implies, taking into account that $y, y^{q^n}, y^{q^{m+n}}$ and $y^{q^{3m}}$ are pairwise distinct modulo $y^{q^{4m}} - y$, that

$$a_0 = a_0^{q^{2m}}.$$

From the last equality and from (4.13), since $\gcd(n, m) = 1$, it follows $\mathcal{N}_m(\mathbb{B}) = F_{q^2}$.

On the other hand, the right nucleus of \mathbb{B} is the largest field $\mathcal{N}_r(\mathbb{B})$ of the space $\mathbb{V} = \text{End}_{\mathbb{F}_q}(\mathbb{F}_{q^{4m}})$, whose elements $\phi: x \mapsto \sum_{i=0}^{4m-1} a_i x^{q^i}$, with $a_i \in \mathbb{F}_{q^{4m}}$, satisfy the property $\phi \circ \varphi_y \in \mathcal{C}$, for each $\varphi_y \in \mathcal{C}$. Arguing as above we get $\mathcal{N}_r(\mathbb{B}) = F_q$. \square

In [6, Thm. 7], it has been shown that a \mathcal{B} presemifield of order q^{4m} , $q = p$ an odd prime, $n = 2$ and $m > 1$ odd, is not isotopic to a Generalized twisted field. By using the previous theorem we can now prove the following

Corollary 4.6. *A Bierbrauer presemifield of order q^4 (i.e., $m = 1$), q an odd prime power, with Multiplication (4.8) is isotopic to a Dickson semifield.*

A Bierbrauer presemifield of order q^{4m} , q an odd prime power and $m > 1$ odd, with Multiplication (4.8), is isotopic neither to a Dickson semifield, nor to a Generalized twisted field and to any of the known commutative presemifields of characteristic 3 (see Table 1).

PROOF. From Theorem 4.1 a \mathcal{B} presemifield of order q^4 is 2-dimensional over its middle nucleus and 4-dimensional over its center. Hence it is isotopic to a Dickson semifield (see [32] and [8]). If $m > 1$ odd, by Theorem 4.1, comparing the orders and the parameters of the involved presemifields over their middle nucleus and over their center (see Table 1), we get the assertion. \square

Corollary 4.7. *A $\overline{BH}(q, \ell, d, \beta)$ presemifield of order $q^{2\ell}$, q an odd prime power and $\ell \neq 2k$ with k odd, defined by Multiplication (4.1), is not isotopic to any Bierbrauer presemifield with Multiplication (4.8).*

PROOF. The assertion again follows by comparing the dimensions of the involved presemifields over their middle nucleus and over their center (see Table 1). \square

4.3. The nuclei of Zha–Kyureghyan–Wang presemifields. Set $g = \gcd(s, t)$, then $s = hg$ and $t = ng$ with $\gcd(h, n) = 1$. Then the multiplication of a Zha–Kyureghyan–Wang presemifield $\mathbb{ZKW} = (\mathbb{F}_{q^{3h}}, +, *)$, $q = p^g$ odd prime power, can be rewritten as

$$(4.14) \quad x \star y = y^{q^n} x + y x^{q^n} - v(y^{q^{h+n}} x^{q^{2h}} + y^{q^{2h}} x^{q^{h+n}}),$$

where $v = u^{q^h - 1}$, u a primitive element of $\mathbb{F}_{q^{3h}}$, and $0 < n < 3h$ such that h is odd. Hence, by Corollary 2.6, all the nuclei and the center of a \mathcal{ZKW} presemifield contain a field of order q . Moreover this multiplication gives rise to a \mathcal{ZKW} presemifield if either

$$(4.15) \quad h + n \equiv 0 \pmod{3}$$

or

$$(4.16) \quad q \equiv 1 \pmod{3}.$$

If $h = 1$ and $n = 2$, by the form of Multiplication (4.14) it is clear that a \mathcal{ZKW} presemifield of order q^3 is isotopic to a Generalized twisted field.

If $h = n = 1$ only Condition (4.16) can be realized. Arguing as in Theorem 4.5 and taking into account that $v^{q^2 + q + 1} = 1$ and that $q \equiv 1 \pmod{3}$, it can be proven that in this case the nuclei and the center have all order exactly q . Hence also in this case, by the classification result of Menichetti [30], the \mathcal{ZKW} presemifield is isotopic to a Generalized twisted field.

More generally, in [26, Thm. 10], using an isotopy form, it has been proven that a \mathcal{ZKW} presemifield of order q^{3h} , $h > 1$ odd, satisfying Condition (4.15) has middle nucleus of order q . Using similar techniques as in Theorem 4.5 it can be proven that also the center of a \mathcal{ZKW} presemifield has order q . In both cases the arguments do not involve the congruences (4.15) and (4.16). Hence we obtain

Theorem 4.8. *A \mathcal{ZKW} presemifield of order q^{3h} , q an odd prime power and h an odd integer, with Multiplication (4.14), has middle nucleus and center both of order q .* \square

Corollary 4.9. *A \mathcal{ZKW} presemifield of order q^3 , q an odd prime power, with Multiplication (4.14), is isotopic to a Generalized twisted field.*

A \mathcal{ZKW} presemifield of order q^{3h} , $q > 3$ an odd prime power and $h > 1$ odd integer, with Multiplication (4.14), is not isotopic to any known presemifield.

PROOF. The first part has been proven above. By [26, Cor. 3], a ZKW presemifield of order q^{3h} , $q > 3$ an odd prime power and $h > 1$ odd integer, is isotopic neither to a Dickson semifield nor to a Generalized twisted field and, by Table 1, it is not isotopic to any presemifield with characteristic 3. Moreover, by Theorems 4.1, 4.5 and 4.8, a ZKW presemifield is isotopic neither to a \mathcal{BH} presemifield nor a \mathcal{B} presemifield by comparing the dimensions of the involved presemifields over their center. \square

The following table summarizes the state of the art on the presently known commutative presemifields whose multiplication are written pointing out their center. In this table we have also written the multiplication and the parameters of some presemifields very recently constructed in [34].

TABLE 1. Commutative proper presemifields of odd characteristic

TYPE	SIZE	$ \mathcal{K} $ $ \mathbb{N}_m $	MULTIPLICATION	EXIS. RESULTS	REFER.
\mathcal{D}	$q^{2k}, k > 1$ odd	q q^k	$(a, b) \star (c, d) = (ac + jb^\sigma d^\sigma, ad + bc)$ where $\sigma \neq 1$ \mathbb{F}_q -autom. of \mathbb{F}_{q^k} and j nonsquare in \mathbb{F}_{q^k}	$\exists \forall q$ odd,	[17], [18], [19]
\mathcal{A}	$q^t, t > 1$ odd	q q	$x \star y = x^\alpha y + xy^\alpha,$ where $\alpha : x \mapsto x^{q^n}$ \mathbb{F}_q -autom. of \mathbb{F}_{q^t} , $\alpha^2 \neq 1$ and $\frac{t}{\gcd(t, n)}$ odd	$\exists \forall q$ odd,	[2], [3]
\mathcal{ZKW}	$q^{3h}, h > 1$ odd	q q	$x \star y = x^{q^n} y + xy^{q^n} - u^{q^h-1} (x^{q^{2h}} y^{q^{h+n}} + y^{q^{2h}} x^{q^{h+n}})$ where $0 < n < 3h$, $(h, n) = 1$ and u prim. elem. of $\mathbb{F}_{q^{3h}}$	$\exists \forall q$ odd, $n + h \equiv 0 \pmod{3}$ $\exists \forall q$ odd : $q \equiv 1 \pmod{3}$	[3], [6], [5]
\mathcal{B}	$q^{4m}, m > 1$ odd	q q^2	$x \star y = x^{q^n} y + xy^{q^n} - u^{q^m-1} (x^{q^{3m}} y^{q^{m+n}} + y^{q^{3m}} x^{q^{m+n}})$ where $0 < n < 4m$, n even, $\gcd(m, n) = 1$ and u prim. elem. of $\mathbb{F}_{q^{4m}}$	$\exists \forall q \equiv 1 \pmod{4},$	[6], [5]
\mathcal{BH}	$q^{2\ell}, \ell > 2$	q q^2	$x \star y = xy^{q^\ell} + x^{q^\ell} y + [\beta(xy^{q^d} + x^{q^d} y) + \beta^{q^\ell}(xy^{q^d} + x^{q^d} y)^{q^\ell}] \omega$ where $0 < d < 2\ell$, $\gcd(\ell, d) = 1$, $\ell + d$ odd, β nonsquare of $\mathbb{F}_{q^{2\ell}}$ and $\omega^{q^\ell} = -\omega$	$\exists \forall q$ odd,	[18], [26], [7]
\mathcal{ZP}	$q^{2\ell}, \ell > 2$	q q^2 (if $\sigma = 1$) q q (if $\sigma \neq 1$)	$(a, b) \star (c, d) = (ac^{q^n} + a^{q^n} c + \alpha(bd^{q^n} + b^{q^n} d)^\sigma, ad + bc),$ where $\sigma : x \mapsto x^{q^t}$ autom. of \mathbb{F}_{q^ℓ} , $\gcd(\ell, n, t) = 1$, $\frac{\ell}{\gcd(\ell, n)}$ odd and α nonsquare of \mathbb{F}_{q^ℓ}	$\exists \forall q$ odd,	[34]
\mathcal{CG}	$3^{2s}, s \geq 3$	3 3^s	$(a, b) \star (c, d) = (ac + jbd + j^3(bd)^9, ad + bc + j(bd)^3)$ j nonsquare in \mathbb{F}_{3^s}		[11]
\mathcal{G}	$3^{2r}, r \geq 3$ odd	3 3	$(a, b) \star (c, d) = (ac - b^9 d - bd^9, ad + bc + (bd)^3)$		[21]
$\mathcal{CM}/\mathcal{DY}$	$3^e, e \geq 5$ odd	3 3	$x \star y = x^9 y + xy^9 \pm 2x^3 y^3 - 2xy$		[14], [20], [12]
$\mathcal{PW}/\mathcal{BLP}$	$3^{10},$	3 3^5	$(a, b) \star (c, d) = (ac + (bd)^9, ad + bc + (bd)^{27})$		[31], [4]
\mathcal{CHK}	$3^8,$	3 3^2	$x \star y = xy + L(xy^9 + x^9 y - xy - x^9 y^9) + x^{243} y^3 + x^{81} y - x^9 y + x^3 y^{243} + xy^{81} - xy^9$ where $L(x) = x^{3^5} + x^{3^2}$		[13]

Some explanatory comments on the above table are needed. The sizes of the middle nucleus and the center of a commutative (pre)semifield belonging to one of the families \mathcal{D} , \mathcal{A} , \mathcal{ZKW} , \mathcal{B} , \mathcal{BH} , \mathcal{CG} , \mathcal{G} , $\mathcal{CM}/\mathcal{DY}$, $\mathcal{PW}/\mathcal{BCP}$, \mathcal{CHK} and \mathcal{ZP} are listed in the middle columns. The fifth column contains the existence results of commutative presemifields belonging to the above families.

4.4. Final remarks. By comparing the dimensions of the commutative presemifields over their middle nucleus and their center, taking into account their characteristic and using Corollaries 4.3, 4.6, 4.7 and 4.9, it follows that the family of \mathcal{ZKW} presemifields of order q^{3h} (with $h > 1$) and the family of \mathcal{BH} presemifields of order $q^{2\ell}$ (with $\ell > 2$) are not isotopic and they are actually new. More precisely, for $q > 3$, these presemifields are not isotopic to any previously known. Regarding the family of \mathcal{B} presemifields, so far it is not still clear whether it contains new examples of presemifields. Indeed, by Table 1 and by comparing the parameters, it is not possible to exclude the possibility that a \mathcal{B} presemifield turns out to be isotopic to a \mathcal{BH} presemifield. As well as, it remains to investigate whether a $\mathcal{CM}/\mathcal{DY}$ presemifield of order 3^n , $n \equiv 0 \pmod{3}$ could be isotopic to a \mathcal{ZKW} presemifield and whether the \mathcal{CHK} presemifield belongs, up to isotopy, to the family of \mathcal{BH} presemifields.

Finally in [34], the authors presented a family of presemifields (the \mathcal{ZP} presemifields) of order $q^{2\ell}$ and center of order q , computing their nuclei. Moreover, they show that, when $\sigma = id$, in some cases, the \mathcal{BH} presemifields are contained, up to isotopisms, in the family of \mathcal{ZP} presemifields, whereas when $\ell > 3$ is odd and $q \equiv 1 \pmod{4}$ the latter family contains presemifields which are non isotopic to any previously known. Obviously, it would be interesting to complete the study of the isotopisms between these two last mentioned families of presemifields for each value of ℓ (odd or even) and for each odd characteristic.

References

- [1] A.A. Albert, *Finite division algebras and finite planes*, Proc. Symp. Appl. Math., **10** (1960), 53–70.
- [2] A.A. Albert, *Generalized Twisted Fields*, Pacific J. Math, **11** (1961), 1–8.
- [3] A.A. Albert, *Isotopy for generalized Twisted Fields*, An. Acad. Brasil. Ciênc., **33** (1961), 265–275.
- [4] L. Bader, G. Lunardon, I. Pinneri, *A new semifield flock*, J. Combin Theory Ser. A, **86** (1999), 49–62.
- [5] J. Bierbrauer, *New commutative semifields and their nuclei*, Proceedings of AAEECC-18 (Tarragona, Spain), M. Bras-Amorós and T. Høholdt (Eds), Lecture Notes in Computer Science, **5527** (2009), 179–185.
- [6] J. Bierbrauer, *New semifields, PN and APN functions*, Designs, Codes, Cryptogr., **54** (2010), 189–200.
- [7] J. Bierbrauer, *Commutative semifields from projection mappings*, Designs, Codes, Cryptogr., to appear (available online 5 November 2010).
- [8] A. Blokhuis, M. Lavrauw, S. Ball, *On the classification of semifield flocks*, Adv. Math., **180** (2003), 104–111.
- [9] L. Budaghyan, T. Helleseht, *New Perfect Nonlinear Multinomials over $\mathbb{F}_{p^{2k}}$ for any odd prime p* , Lecture Notes in comput. Sci., vol. 5203, SETA (2008), 403–414.
- [10] L. Budaghyan, T. Helleseht, *New commutative semifields defined by PN multinomials*, Cryptogr. Commun., **3** No.1 (2011), 1–16.
- [11] S.D. Cohen, M.J. Ganley, *Commutative semifields, two-dimensional over their middle nuclei*, J. Algebra, **75** (1982), 373–385.
- [12] R.S. Coulter, M. Henderson, *Commutative presemifields and semifields*, Adv. Math., **217** (2008), 282–304.

- [13] R.S. Coulter, M. Henderson, P. Kosick, *Planar polynomials for commutative semifields with specified nuclei*, Des. Codes Cryptography, **44** (2007), 275–286.
- [14] R.S. Coulter, R.W. Matthews, *Planar functions and planes of Lenz–Barlotti clas II*, Des. Codes Cryptography, **10** (1997), 167–184.
- [15] J. De Beule, L. Storme (Editors): *Current research topics in Galois Geometry*, NOVA Academic Publishers, to appear.
- [16] P. Dembowski, *Finite Geometries*, Springer Verlag, Berlin, 1968.
- [17] L.E. Dickson, *On finite algebras*, Göttingen nachrichtung, (1905), 358–393.
- [18] L.E. Dickson, *Linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc., **7** (1906), 370–390.
- [19] L.E. Dickson, *On commutative linear algebras in which division is always uniquely possible*, Trans. Amer. Math. Soc., **7** (1906), 514–522.
- [20] C. Ding, J. Yuang, *A new family of skew Paley–Hadamard difference sets*, J. Combin. Theory, Ser. A, **113** (2006), 1526–1535.
- [21] M.J. Ganley, *Central weak nucleus semifields*, European J. Combin., **2** (1981), 39–347.
- [22] W.M. Kantor, *Commutative semifields and symplectic spreads*, J. Algebra, **270** (2003), 96–114.
- [23] D.E. Knuth, *Finite semifields and projective planes*, J. Algebra, **2** (1965), 182–217.
- [24] M. Lavrauw, O. Polverino, *Finite semifields*. Chapter in Current research topics in Galois Geometry (J. De Be Storme, Eds.), NOVA Academic Publishers, to appear.
- [25] G. Lunardon, *Symplectic spreads and finite semifields*, Designs, Codes, Cryptogr., **44** (2007), 39–48.
- [26] G. Lunardon, G. Marino, O. Polverino, R. Trombetti, *Symplectic Semifield Spreads of $PG(5, q)$ and the Veronese Surface*, Ricerche di Matematica, **60** No.1 (2011), 125–142.
- [27] D.M. Maduram, *Transposed Translation Planes*, Proc. Amer. Math. Soc., **53** (1975), 265–270.
- [28] G. Marino, O. Polverino, *On isotopisms and strong isotopisms of commutative presemifields*, submitted (arXiv:1105.5940).
- [29] G. Marino, O. Polverino, R. Trombetti, *Towards the classification of rank 2 semifields 6-dimensional over their center*, Designs, Codes, Cryptogr., **61** No.1 (2011), 11–29.
- [30] G. Menichetti, *On a Kaplansky conjecture concerning three-dimensional division algebras over a finite field*, J. Algebra, **47** (1977), 400–410.
- [31] T. Penttilä, B. Williams, *Ovoids of parabolic spaces*, Geom. Dedicata, **82** (2000), 1–19.
- [32] J.A. Thas, *Generalized quadrangles and flocks of cones*, Europ. J. Combin., **8** (4) (1987), 441–452.
- [33] Z. Zha, G.M. Kyureghyan, X. Wang, *Perfect nonlinear binomials and their semifields*, Finite Fields Appl., **15** No. 2 (2009), 125–133.
- [34] Y. Zhou, A. Pott, *A new family of semifields with 2 parameters*, submitted (arXiv:1103.4555).

DIPARTIMENTO DI MATEMATICA, SECONDA UNIVERSITÀ DEGLI STUDI DI NAPOLI, I–81100 CASERTA, ITALY

E-mail address: `giuseppe.marino@unina2.it`

DIPARTIMENTO DI MATEMATICA, SECONDA UNIVERSITÀ DEGLI STUDI DI NAPOLI, I–81100 CASERTA, ITALY

E-mail address: `olga.polverino@unina2.it`